UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,309	02/19/2004	Ari Juels	4414-35	7635

7590 08/02/2005

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
BANGACHON, WILLIAM L	
ART UNIT	**PAPER NUMBER**
2635	

DATE MAILED: 08/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/782,309	JUELS, ARI	
	Examiner	Art Unit	
	William Bangachon	2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *17-19,21 and 22* is/are allowed.

6)☒ Claim(s) *1-16,20 and 23-33* is/are rejected.

7)☒ Claim(s) *17-19, 21-22* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5/11/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 5/11/2005 have been fully considered but they are not persuasive.

2. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., **the term pseudonym is defined as including device-identifying information transmitted by an RFID device** [page 3, 4th – 5th paragraph; page 4, 2nd – 3rd paragraph]; **one-time pad is a type of cryptographic construct** [page 6, 6th paragraph]) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

3. The Examiner respectfully traverse applicant's arguments (although not claimed) that, **"the secret value used in the system of Hughes is not a pseudonym"** [page 4, 1st – 2nd paragraph]. Page 8 of the applicant's specification clearly states, **"seeds, secrets, hashes or other information are used to generate the pseudonyms"**. There is no indication in the claims as to the type of pseudonym used. Clearly, the secret value used in the system of Hughes is device-identifying information because only the device knows this secret value. Further, the Examiner respectfully traverse

applicant's arguments (although not claimed) that "the index designators of Dannhaeuser do not relate to any aspect of cryptography" [page 6, 6th paragraph] in that each code combination sequence (indexed values) can be stored in the form of algorithm which is executed by the respective processor to determine the appropriate code or code number to be transmitted or matched {Dannhaeuser, col. 2, lines 63-68}. Obviously, this is another form or variation of a cryptographic technique, for the purpose of saving memory space.

4. In response to applicant's argument [page 3, 2nd paragraph; page 5] that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the systems of Hughes are in the same field of endeavor, particularly "wireless communication". And they are in the same problem solving area, specifically "code protection of wireless signals". The suggestion to combine "transmitting different ones of the pseudonyms" in the system of Hughes, as taught by Dannhaeuser, because it provides security to a wireless communication by foiling attempts of code grabbers from copying and re-using a single transmitted pseudonym to be used in unauthorized accesses.

5. In response to applicant's argument that "if the Dannhaeuser code rotation were applied to the secret value 66 of Hughes, it would appear to be very difficult and highly impractical to coordinate such secret key value rotation between all the tags and the reader" [page 5, last paragraph], the fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985). Further, Hughes teaches that the authentication system can realized with the use of multiple keys, both public and private {col. 7, lines 48-58}, which is obviously another form of code rotation.

6. In response to applicant's argument [page 6, 2nd paragraph] that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

7. The Examiner inadvertently omitted the rejection of claim 31 in the last Office action. Claim 31 recites the combination of claims 1 and 3, which was rejected in that

Office action. Therefore, the substance of claim 31 had previously been addressed. The rejection to claim 31 is now included in this Office action.

8. Based on the above observations, the recited claim limitations are generally broader than what applicant argues. Therefore, the rejection to claims 1-16, 20, 23-33 and objection to claims 17-19 and 21-22 as being dependent upon a rejected base claim, is maintained in this Office action.

Drawings

9. Applicant's arguments with respect to the drawings have been fully considered and are persuasive. The objection of the drawings under 37 CFR 1.83(a) has been withdrawn.

Claim Objections

10. Claims 17-19 and 21-22 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

13. Claims 1-2, 4-8, 20, 23-25, 30, and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP 6,842,106 (Hughes et al) in view of USP 4,928,098 (Dannhaeuser).

In claims 1 and 2, Hughes teach of a method for use in an RFID system comprising at least one or more tags 44 (RFID device) and at least one or more reader/s (32) which communicates with the tag {abstract}, the method comprising the steps of:

associating a plurality of pseudonyms (key value) with the tag (RFID device) {col. 5, lines 47-50; col. 6, lines 32-33, lines 64-65; col. 7, lines 51-53}; and

transmitting from the tag (RFID device) pseudonyms in response to different reader queries of the RFID device {col. 6, lines 15-18, lines 27-28}. In this case, the pseudonyms are converted to pseudo random number based on the key value {col. 6, lines 18-26};

wherein an authenticator (authorized verifier) is able to determine that the different transmitted pseudonyms (key value) are associated with the same tag {col. 5, lines 61-64; col. 6, lines 42-46}. In this case, the reader doubles as an authenticator {col. 6, lines 16-18}.

Although Hughes teaches of using multiple key values {col. 7, lines 52-58}, Hughes does not disclose expressly "transmitting different ones of the pseudonyms". Dannhaeuser, in the same field of endeavor (wireless communication), teach of storing plurality of pseudonyms in tabular form in both a transmitter and receiver (as shown in the table of column 3) wherein the plurality of pseudonyms are cyclically traversed by the transmitter and receiver during transmission {Dannhaeuser, col. 3, lines 1+}. Dannhaeuser teaches that this feature foils attempts of code grabbers from copying and re-using a single transmitted pseudonym to be used in unauthorized accesses {Dannhaeuser, col. 1, lines 26+}. Hughes is concerned with communication security {Hughes, col. 2, lines 29+}. Clearly, the teaching of Dannhaeuser is desirable in the system of Hughes. Therefore, at the time of the invention, it would have been obvious to one of ordinary skill in the art to be transmitting different ones of the pseudonyms in the system of Hughes, as taught by Dannhaeuser, because it provides security to a wireless communication by foiling attempts of code grabbers from copying and re-using a single transmitted pseudonym to be used in unauthorized accesses.

In claims 4, the tag is configured to authenticate itself to an authenticator only after the authenticator has authenticated itself to the tag {Hughes, col. 7, lines 32-47}.

In claim 5, the authenticator authenticates itself to the tag by releasing to the tag a first challenge value (authentication value) unique to a given pseudonym transmitted by the tag {Hughes, col. 7, lines 16-23}.

In claim 6, the tag authenticates itself to the authenticator by releasing to the authenticator a second challenge value (authentication value) unique to a given pseudonym transmitted by the RFID device {Hughes, col. 7, lines 24-31}.

In claim 7, one or more of the pseudonyms each comprise an identifier of the tag {Hughes, col. 6, lines 57-65}. In this case, the tag key value identifies the tag.

In claim 8, the method of claim 1 wherein one or more of the pseudonyms each comprise a portion of an identifier of the RFID device {Hughes, col. 6, lines 60-62}. In this case, the tag key value is convoluted to obscure the key value.

In claim 20, a verifier is configured to store for a given RFID device Tx an address no. (a static identifier idx) corresponding to at least one pseudonym of Tx {Dannhaeuser, Fig. 3}.

In claim 23, a verifier specifies value identifying a particular pseudonym {Dannhaeuser, col. 3, lines 49+}.

In claim 24, the RFID device determines which of the plurality of pseudonyms to transmit responsive to a given reader query based at least in part on timing information {Dannhaeuser, paragraph bridging cols. 3 and 4}.

In claim 25, the method of claim 1 wherein the RFID device incorporates a pseudorandom number generator, where fx(i) represents an output of the pseudorandom number generator for index i, where x is a key value (seed) associated with the RFID device {Hughes, col. 5, lines 53-64}.

Claims 30 and 32 recites a system/apparatus for practicing the method of claim 1 and therefore rejected for the same reasons.

Claim 33 recites the limitations of claim 1 and therefore rejected for the same reasons, further comprising determining utilizing an updateable set of one-time pads (index designators) maintained in the device {Dannhaeuser, col. 4, lines 5-24}.

14. Claims 3 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP 6,842,106 (Hughes et al) in view of USP 4,928,098 (Dannhaeuser), and further in view of USP 6,724,895 (Turner et al).

In claim 3, Hughes does not disclose expressly "the transmitted pseudonyms are authenticated by an authenticator (verifier) other than the reader". Turner, in the same field of endeavor, teaches of having a plurality of readers/verifiers in an RFID system {col. 4, lines 40-42}. Clearly, since a verifier is also a reader, anyone of them is the reader and anyone of them is the verifier {Turner, Figure 1}. And since the reader of Hughes is also an authenticator {Hughes, col. 6, lines, 15-16}, a plurality of readers in the system of Hughes, as evidenced by Turner, would have an authenticator authenticating the transmitted pseudonym that is other than the reader. Therefore, at the time of the invention, it would have been obvious to one of ordinary skill in the art to have a plurality of readers in the system of Hughes, as evidenced by Turner, wherein an authenticator authenticates the transmitted pseudonym that is other than the reader.

Claim 31 recites a system for practicing the combination of method claims 1 and 3 and therefore rejected for the same reasons.

15. Claims 9-16, 14-16, and 26-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP 6,842,106 (Hughes et al) in view of USP 4,928,098 (Dannhaeuser), and further in view of USP 6,225,889 (Furuta et al).

In claims 9-16, although Hughes in view of Dannhaeuser teach that the pseudonyms (key values) are stored in the RFID device as an ordered list of pseudonyms {Hughes, col. 7, lines 52-53; Dannhaeuser, Fig. 3}, Hughes does not

disclose expressly "the step of designating a particular one of the pseudonyms as a current pseudonym and, in response to a given reader query, transmitting the current pseudonym, wherein over a plurality of reader queries the pseudonym designated as the current pseudonym periodically cycles through the list of pseudonyms". Furuta et al, in the same field of endeavor (transponder systems), teach of a method of producing rolling codes between a vehicle transceiver 2 (analogous to the claimed reader) and key transceiver 1 (analogous to the claimed RFID device). The rolling codes are constantly changed by cycling through a different one of a plurality of initial code variables (pseudonym) stored in the memory (5) of the vehicle transceiver 2, shown in Figure 3 {Furuta, col. 5, lines 13-26}. Initially, one of the plurality of the initial code variable stored in the memory (5) of the vehicle transceiver 2 is designated as the current initial code variable, transmitted to the RFID device and stored in the memory of the RFID device (as claimed in 10 and 12) {Furuta, col. 4, lines 17-29}. So that in response to an as needed initial reader query (as claimed in 11), the current initial code variable stored in the memory of the RFID device is used to produce a unique rolling code {Furuta, col. 6, lines 53+} and transmitted to the reader {Furuta, col. 7, lines 11+}. In the case of a mismatched determination, a given period of time is given to a user to transmit another rolling code (as claimed in 13) {Furuta, col. 8, lines 4-11}. Obviously, these features are desirable in the system of Hughes because it provides a high degree of security without compromising system cost, to one of ordinary skill in the art.

In claims 14-16, the initial code variable may be altered sequentially (as claimed in 14) by the reader {Furuta, col. 8, lines 60+}, in response to receipt of refresh information (as claimed in 15) {Furuta, col. 8, lines 18-22}, after the current initial code variable is determined to be invalid (as claimed in 16) {Furuta, col. 7, lines 63+}. Furuta et al teach that the method above is capable of producing rolling codes with a high degree of security using a simple algorithm that do not require large storage capacity {Furuta, col. 1, lines 61-65}. Hughes is concerned with tradeoffs between level of security and system cost {Hughes, col. 7, lines 1-3}. Obviously, these features are desirable in the system of Hughes because it provides a high degree of security without compromising system cost, to one of ordinary skill in the art.

In claim 26, the method of claim 25 wherein the RFID device generates the plurality of pseudonyms as pseudonyms c1 =f(1), c2 =f(2), ..., ck =f(3) {Furuta, col. 8, lines 60-65}.

In claim 27, the method of claim 25 wherein the RFID device and a verifier of the system attempt to maintain a common counter dx unique to the RFID device, and share the seed n {Hughes, col. 5, lines 46-50}.

In claim 28, the method of claim 27 wherein in order to determine which RFID device is associated with a given incoming value g, the verifier performs a lookup in a list {fx (dx)} of current g values for a plurality of RFID devices {Hughes, col. 5, lines 21-

23}. In this case, g=tag identification code. And since there is a plurality of tags {Hughes, col. 5, lines 8-10}, obviously, a list of identification code for each tag is stored in the memory of the authenticator to distinguish which tag has responded to an interrogation signal, to one of ordinary skill in the art.

In claim 29, the method of claim 27 wherein for a given counter value d, the RFID device computes cd=f(bk + d), where b denotes a base value, and the verifier provides a subsequent instruction to the RFID device to increment the base value b {Furuta, col. 6, lines 48-52}.

Conclusion

16. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Examiner Contact Information

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to William Bangachon whose telephone number is (571)-272-3065. The examiner can normally be reached on 4/4/10.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached on (571)-272-3068. The fax phone numbers for the organization where this application or proceeding is assigned is 703-872-9314 for regular and After Final formal communications. The examiner's fax number is (571)-273-3065 for informal communications.

Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-4700.

ALBERT K. WONG
PRIMARY EXAMINER

William L Bangachon
Examiner
Art Unit 2635